VZCZCXRO0168
RR RUEHAG RUEHAST RUEHDA RUEHDBU RUEHDF RUEHFL RUEHIK RUEHKW RUEHLA
RUEHLN RUEHLZ RUEHNP RUEHPOD RUEHROV RUEHSK RUEHSL RUEHSR RUEHVK
RUEHYG
DE RUEHTL #0205/01 2111220
ZNR UUUUU ZZH
R 301222Z JUL 09
FM AMEMBASSY TALLINN
TO RUEHC/SECSTATE WASHDC 0038
INFO EUROPEAN POLITICAL COLLECTIVE
RHMFISS/HQ USEUCOM VAIHINGEN GE
RUEHNO/USMISSION USNATO BRUSSELS BE
RUEHSI/AMEMBASSY TBILISI 0002
RUEHTL/AMEMBASSY TALLINN

UNCLAS SECTION 01 OF 03 TALLINN 000205

SENSITIVE
SIPDIS
STATE FOR INR CYBER MICHELLE MARKOFF

E.O. 12958: N/A
TAGS: PGOV PTER PREL NATO EN
SUBJECT: ESTONIA?S NATIONAL CYBER DEFENSE AGENDA

REFTEL A: 2007 TALLINN 366
B: 2008 TALLINN 428

¶1. (U) SUMMARY: Unprecedented and wide-spread cyber attacks in April/May 2007 galvanized Estonia to think strategically about the security of its critical IT infrastructure. Estonia's brainstorming has culminated in a new national cyber defense policy for 2009-2011, focused on strengthening ties between the private sector and government, greater personal computer security responsibility among the populace, and the need for comprehensive international legislation on cyber security within the framework of multi-national organizations. President Obama's recent declaration that cyber security was a high priority for the U.S. has the Government of Estonia looking for areas of increased bilateral cooperation with the U.S. in cyber security. END SUMMARY.

Implementing Cyber Security

¶2. (U) Even prior to April 2007, Estonia was "cyber-savvy," with a small, highly- educated and IT-focused population well-suited for developing high-tech industry and internet innovation. In fact, Estonia's Cooperative Cyber Defense Center of Excellence(CCD COE), which was accredited by NATO in 2008, began building an international reputation in 2003. The April/May 2007 cyber attacks, however, underscored the vulnerability of Estonia's government and private sector Internet infrastructure to cyber warfare (Ref A).

¶3. (SBU) In the wake of the attacks, the GOE directed the Ministry of Defense, in cooperation with the Ministry of Education and Research, the Ministry of Justice, the Ministry of Economic Affairs and Communications, the Ministry of Internal Affairs and the Ministry of Foreign Affairs, to develop a "Cyber Security Strategy for 2008-2013." The inter-agency committee tasked with developing the Strategy also included information security experts from the Estonian private sector. This strategy, intended to safeguard Estonia from future attacks and serve as a model for other countries, was formally unveiled to the public in May 2008. However, the budget crisis in Estonia delayed implementation for more than a year.

¶4. (SBU) In May 2009, the GOE endorsed a plan to implement its national cyber security strategy for the period 2009-2011. The plan calls for a "graduated" system of security measures, development of Estonian expertise in information security, development of an appropriate regulatory and legal framework, and promotion of international cooperation toward achieving global cyber security. The strategy rests on the premise that improved security can only be achieved through international cooperation between nations and with the private sector, and

that national cyber security measures must be made visible to encourage international investment.

Enhancing Public-Private Cooperation

¶5. (SBU) In order to achieve the goals outlined in the plan, the GOE will establish a "cyber security critical information infrastructure security unit" this year under the authority of the Ministry of Economic Affairs and Communications. Our GOE cyber security contacts have told us that the mandate of this body will be to liaise with the private sector and oversee security measures and information security across the GOE. The aim of this cross-cutting mandate will be to address key deficiencies highlighted by the 2007 attacks, such as the limited role played by the private sector in national cyber defense.

¶6. (SBU) As one example of how the private sector and the government should join forces, two companies (Linx Telecom and Elion) provide Estonia's backbone connection to the internet. Linx Network Architect Marko Veelma and Country Manager Erki Uvra told poloff they have only occasionally consulted with Ministry of Defense working groups on cyber defense strategy. Instead, they described parallel, rather than integrated, approaches to security among the GOE, banks and private ISPs. Urva and Veelma noted that during the April 2007 massive denial of service (DOS) attacks on banks and government websites in Estonia, Linx Telecom itself was barely affected; online news services that used their servers for internet hosting, for example, were still accessible outside Estonia,

while banks and GOE websites had to be cut off from the internet outside Estonia. Linx's massive capacity, and ability to re-route traffic via neighboring Swedish and Finnish networks, means that a massive DOS attack on a particular user of their network may register as barely a blip to the overall system. Both the Linx employees and our GOE contacts have told us the government will make use of such resources as it implements its own cyber security plans.

¶7. (U) The 2009-2011 security strategy calls for increased public and private sector cooperation to protect critical information infrastructure, coordinate the distribution of information on cyber threats, and organize security awareness campaigns together with the private sector. The GOE emphasis on this aspect of cyber security is evident in the rhetoric of key Estonian public figures. In a recent key note speech to mark the opening of a cyber defense conference in Tallinn, Estonian Minister of Defense Jaak Aaviksoo stated that cyber security reaches across all fields of cooperation and that a successful strategy will depend heavily on civilian sector contributions. In addition, during a June 2009 trip to Silicon Valley in California to promote Estonian industry, Estonian President Toomas Hendrik Ilves stressed that efficient international cooperation between the private and public sectors is required in order to anticipate cyber threats and to eradicate their consequences.

¶8. (U) Another key tool of the GOE strategy is to raise the awareness and greater personal computer security responsibility of the individual user. In order to achieve this goal, the new strategy foresees the introduction of cyber defense and information security tools at all levels of education, the establishment of minimum requirements for competence in IT security and cyber defense for both public and private sector staff and the organization of an "appropriate evaluation process."

Developing Niche Capabilities

¶9. (SBU) On the international front, the plan envisions a smaller but more defined role for the GOE than in the past. According to Heli Tiirmaa-Klaar, cyber security coordinator at

the Estonian Ministry of Defense, in the immediate aftermath of the 2007 attacks Estonia wanted to become a global leader in cyber security. However, over the course of the past two years, the complexity of cyber security issues has forced the GOE to consider the benefits of identifying a few niche capabilities. In particular, Estonia would like to enhance the profile of the CCD COE. According to Ilmar Tamm, CCD COE director, the main goal of the center is to conduct post-incident analysis and research to identify root causes, motivation and future threats. Currently, seven NATO member states have officially signed on as Sponsoring Nations (the U.S., Turkey, and Hungary are in line to join as Sponsors, with Finland, Norway, and Sweden to join as Cooperative Partners). The GOE wants to expand membership and the manpower available to expand research capabilities.

¶10. (SBU) The cyber security strategy also outlines the importance the GOE places on international cooperation as a key element to increasing national cyber security. Not only does the strategy call for further development of the NATO CCD COE's profile, but for increased focus on raising awareness of cyber security in organizations such as NATO, UN, OSCE, and the OECD (which Estonia hopes to join in 2009). Tiirmaa-Klaar pointed to the number of laws for cyber crime on the books in EU and NATO member states, such as the Council of Europe and EU Conventions on cyber crime, but the comparative dearth of such legislation in other countries. The result of this disparity is that there is no legal basis for criminalizing cyber attacks in many countries. This September, the CCD COE will host a conference in Tallinn intended to raise awareness of the need for increased legislation and make governments aware of what binding international agreements and laws can do for them.

An Opportunity for Enhanced Cooperation with the U.S.

¶11. (SBU) President Obama's elevation of the cyber threat to a primary national/international security challenge has the GOE considering possibilities for increased Estonia-U.S. bilateral cooperation in cyberspace. Martin Paas, cyber policy advisor

at the Estonian Ministry of Interior, told us that the GOE would be very interested in developing ties between U.S. and Estonian cyber security experts dealing with restricted or classified networks, an area Paas cites as being underdeveloped. Paas also communicated the GOE's interest in working with the U.S. to create a training curriculum for the protection of networks. According to Paas, the rapid development of networks and the implementation of different technical solutions have created new types of threats and challenges which can be tackled in close cooperation with partners, both via exchange of experience and creation of training programs.

¶12. (SBU) Heli Tiirmaa-Klaar stated that a high priority for the GOE is training, education and research in information security. Tiirmaa-Klaar suggested that, within the confines of the newly signed but so far un-ratified Science and Technology Agreement (ref B), the USG and GOE could pursue bilateral training and education cooperation, such as academic studies, on-the-job training and expert exchanges.

¶13. (SBU) COMMENT: Cyber security is a key MSP goal, and a big piece of our agenda with the Estonians. Getting the U.S. through the final couple of steps and into the CCD COE as a sponsoring nation is a high priority for us, as it will increase our influence with Estonia and other cyber-minded nations. We also promote deepened ties between and among government agencies and the private sector, and have used the Overseas Security Advisory Committee (OSAC) as a vehicle for supporting public-private discussions of cyber security. The nexus between cyber security and digital piracy is another target area where we and Estonia have overlapping interests. As Estonia develops its niche capabilities, we anticipate

being part of the discussion about what makes sense. The prospects are bright: Estonia is viewed by many as a post-Soviet success story whose capabilities, influence and advice are held in high regard internationally. Estonia's eagerness to identify new areas of bilateral cooperation is an excellent opportunity for the U.S. to participate in the development of cyber security policy and further enhance an already solid bilateral partnership. END COMMENT.
DECKER